

Manuel de la sécurité intégrée HP ProtectTools

Ordinateurs d'entreprise HP modèle dx5150

Référence : 376352-051

Décembre 2004

Ce manuel contient le mode d'emploi du logiciel permettant de définir les paramètres de configuration de la puce de sécurité intégrée HP ProtectTools.



AVERTISSEMENT : le non-respect de ces instructions expose l'utilisateur à des risques potentiellement très graves.



ATTENTION : le non-respect de ces instructions présente des risques, tant pour le matériel que pour les informations qu'il contient.

Manuel de la sécurité intégrée HP ProtectTools

Première édition (décembre 2004)
Référence : 376352-051

Table des matières

Sécurité intégrée HP ProtectTools

Sécurité intégrée HP ProtectTools

Le gestionnaire de sécurité intégrée HP ProtectTools est un logiciel qui permet de configurer le logiciel de sécurité intégrée HP ProtectTools. Ce gestionnaire est une interface à ligne de commande permettant d'accéder aux différentes options du logiciel HP ProtectTools. Le logiciel HP ProtectTools consiste en une série d'utilitaires comprenant PSD (Personal Secure Drive), l'interface de la puce de cryptage/TPM, la migration de la sécurité, la création d'archives et le contrôle des mots de passe.

Conditions requises

Pour pouvoir utiliser les fonctions de sécurité, vous devez disposer des outils suivants :

- Logiciel de sécurité intégrée HP ProtectTools
- Gestionnaire de sécurité intégrée HP ProtectTools
- Puce de sécurité intégrée HP ProtectTools installée sur la carte mère

Pour plus d'informations sur la mise en œuvre de la solution de sécurité intégrée, reportez-vous à la section "Procédures de configuration" page 8.

Concepts fondamentaux de la sécurité intégrée HP ProtectTools

Cette section contient des informations de haut niveau sur les concepts que vous devez comprendre pour pouvoir utiliser la sécurité intégrée HP ProtectTools et le gestionnaire de sécurité HP ProtectTools.

Puce de sécurité intégrée HP ProtectTools

La puce de sécurité intégrée est un composant matériel caractérisé par des fonctions de sécurité et de cryptage et doté d'une capacité de stockage inviolable pour la protection des clés privées et publiques. Cette puce est installée en usine et son retrait est exclusivement réservé aux mainteneurs agréés HP.

Unité personnelle sécurisée

L'unité personnelle sécurisée (PSD, Personal Secure Drive) est une caractéristique de la sécurité intégrée. Il s'agit d'une unité virtuelle qui est créée sur le disque dur pendant l'initialisation de l'utilisateur de la sécurité intégrée HP ProtectTools. Cette unité sécurisée offre une capacité de stockage protégée pour les données sensibles. Elle vous permet de créer des fichiers et des dossiers et d'y accéder de la même manière que pour des unités de disque ordinaires.

L'accès à l'unité PSD nécessite d'avoir physiquement accès à l'ordinateur sur lequel elle réside et de connaître le mot de passe PSD. Lorsque vous entrez le mot de passe PSD, l'unité PSD apparaît et vous pouvez accéder aux fichiers qu'elle contient. Ces fichiers restent accessibles tant que la session PSD reste ouverte ; une fois la session fermée, l'unité PSD disparaît automatiquement Il n'est pas possible d'accéder à une unité PSD par l'intermédiaire d'un réseau.

Des données cryptées sont stockées sur le PSD. Les clés de cryptage des fichiers sont stockées sur la puce de sécurité intégrée HP ProtectTools ; elles sont ainsi “verrouillées” à l'ordinateur et les utilisateurs non autorisés n'y ont pas accès. Les données protégées sont donc uniquement accessibles sur l'ordinateur cible.

Email

La messagerie sécurisée est une autre importante fonctionnalité de la sécurité intégrée. Elle permet d'échanger des informations confidentielles et d'assurer que leur authenticité est maintenue pendant le transfert. La messagerie sécurisée permet de :

- Sélectionner un certificat de clé publique émis par un organisme de certification.
- Signer numériquement des messages.
- Chiffrer des messages.

La sécurité intégrée et le gestionnaire de sécurité HP ProtectTools améliorent la sécurisation des messages par une protection supplémentaire de la clé utilisée pour chiffrer, déchiffrer et signer numériquement les messages. La sécurité du courrier électroniques est améliorée avec les systèmes de messagerie suivants :

- Microsoft Outlook Express (version 4 ou supérieure)
- Microsoft Outlook 2000
- Microsoft Outlook 2002
- Netscape Messenger 4.79
- Netscape Messenger 7.0

Pour le mode d'emploi des systèmes de messagerie, reportez-vous à la rubrique sur l'intégration de la messagerie dans l'aide de la sécurité intégrée HP ProtectTools.

Système de fichiers EFS

Le système de fichiers EFS (Enhanced Encrypted File System) est le service de chiffrement des fichiers prévu dans Microsoft Windows 2000 et Windows XP édition professionnelle. Le système EFS assure la protection des données à l'aide des fonctions suivantes :

- Cryptage des fichiers par l'utilisateur au moment de l'enregistrement sur disque
- Accès rapide et simple au fichiers cryptés
- Cryptage automatique (et transparent) des données
- Possibilité pour l'administrateur système de récupérer des données cryptées par un autre utilisateur

La sécurité intégrée et le gestionnaire de sécurité HP ProtectTools améliorent le système EFS par une protection supplémentaire de la clé utilisée pour chiffrer et déchiffrer les données.

Pour plus d'informations sur le système EFS, reportez-vous à l'aide en ligne du système d'exploitation.

Utilisateurs et administrateurs

Utilisateurs

Les utilisateurs disposent d'un accès de base à la sécurité intégrée et peuvent :

- envoyer et recevoir des messages électroniques chiffrés
- chiffrer des fichiers et des dossiers
- initialiser une clé personnelle de base
- créer, supprimer ou modifier un compte personnel dans le cadre de la sécurité intégrée
- configurer, créer, utiliser et supprimer des unités PSD

Administrateurs

Les administrateur initialisent la solution de sécurité intégrée sur un ordinateur et peuvent :

- configurer la machine locale et les règles d'utilisation de la sécurité intégrée
- préparer des clés et des certificats utilisateur pour le transfert
- changer le mot de passe propriétaire de la sécurité intégrée
- désactiver et activer la sécurité intégrée
- autoriser des ordinateurs de destination pour le transfert de la clé et du certificat utilisateur
- récupérer des données stockées et cryptées à l'aide de la sécurité intégrée

Pour plus d'informations sur les utilisateurs et les administrateurs de la sécurité intégrée, reportez-vous à l'aide en ligne du système d'exploitation. Pour plus d'informations sur les propriétaires de la sécurité intégrée, reportez-vous à l'aide de la sécurité intégrée HP ProtectTools.

Certificats numériques

Les certificats numériques sont une forme de clé électronique confirmant l'identité d'une personne ou d'une société. Ces clés sont des nombres ou des chaînes de caractères uniquement connus de l'expéditeur et/ou du destinataire. Le propriétaire d'un certificat numérique est authentifié par une signature électronique jointe aux messages électroniques envoyés par ce même propriétaire.

Les certificats numériques sont émis par un organisme de certification et contiennent les informations suivantes :

- Clé publique du propriétaire
- Nom du propriétaire
- Date d'expiration du certificat numérique
- Numéro de série du certificat numérique
- Nom de l'organisme qui a émis le certificat numérique
- Signateur numérique de l'organisme de certification qui a émis le certificat numérique

Signature numérique

Une signature numérique présente le nom de l'organisme émetteur du certificat numérique. Elle est utilisée pour :

- vérifier l'identité de l'émetteur d'un document numérique.
- certifier que le contenu n'a pas été modifié après signature numérique du document par l'émetteur.

Pour plus d'informations sur les signatures numériques, reportez-vous à l'aide en ligne du système d'exploitation.

Clés publiques et clés privées

La sécurité intégrée se base sur la cryptographie asymétrique pour chiffrer les informations ; cette méthode requiert deux clés : une clé privée et une clé publique.

Une clé publique peut être communiquée librement à un grand nombre de personnes, tandis qu'une clé privée est conservée par une seul utilisateur.

Par exemple, pour envoyer un message chiffré à l'utilisateur B, l'utilisateur A utilise la clé publique de l'utilisateur B (communiquée librement) pour chiffrer le contenu de son message. Comme l'utilisateur B est le seul détenteur de la clé privée correspondante, il est le seul à pouvoir déchiffrer le contenu du message de l'utilisateur A.

La technique de la clé publique permet de transmettre des informations privées par l'intermédiaire d'un réseau public, d'utiliser des signatures numériques pour garantir l'authenticité des messages électroniques et d'authentifier un serveur et un client.

Restauration de secours

Le fichier d'archivage ERA (Emergency Recovery Archive) créé par l'administrateur lors de la configuration de la sécurité intégrée est une fichier de secours contenant des données sensibles à propos de l'ordinateur, des utilisateurs de celui-ci, des clés privées utilisées pour protéger les données chiffrées ou privées. En cas de défaillance du système, ces données sensibles sont nécessaires pour rétablir l'accès aux données protégées.

La clé de restauration ERT (Emergency Recovery Token), également créée par l'administrateur pendant la configuration de la sécurité intégrée, est un fichier contenant les clés utilisées pour protéger les données du fichier de restauration ERA. Cette clé est indispensable pour accéder au fichier d'archivage. L'accès à la clé de restauration ERT est protégé par un mot de passe. Ce mot de passe est requis lorsque le système de sécurité intégrée doit être restauré.

Règles

Le comportement d'un ordinateur ou d'un logiciel est régi par des règles. Les règles assurant un usage cohérent de la sécurité intégrée au sein d'une entreprise sont généralement définies par l'administrateur système. Ces règles sont de deux types : les règles machine et les règles utilisateur.

Règles machine

Les règles machine régissent le comportement général de la sécurité intégrée se rapportant à un ordinateur spécifique.

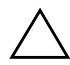
Règles utilisateur

Les règles utilisateur définissent les droits de l'utilisateur de la sécurité intégrée.

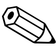
Pour plus d'informations sur les règles machine et utilisateur, reportez-vous à l'aide de la sécurité intégrée HP ProtectTools.

Procédures de configuration

Pour activer et initialiser la puce de sécurité intégrée à l'aide de l'utilitaire Computer Setup dans le BIOS système, procédez comme suit :



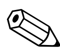
ATTENTION : pour prévenir tout risque, HP recommande que la puce de sécurité intégrée soit immédiatement initialisée par une personne autorisée de l'entreprise (voir étape 4). Si cette précaution n'est pas prise, un utilisateur malveillant, un ver ou virus informatique peuvent prendre possession du système.



Le mot de passe Superviseur BIOS doit être défini dans Computer Setup avant de pouvoir accéder à la puce pour la configurer. Pour plus d'informations cet utilitaire, consultez le *Manuel de l'utilitaire Computer Setup (F10)* sur le *CD Documentation* accompagnant l'ordinateur.

Activation de la puce de sécurité

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter l'ordinateur > Redémarrer**.
2. Dès que l'ordinateur est allumé, appuyez sur la touche **F10** et maintenez-la enfoncée jusqu'à ce que Computer Setup apparaisse.



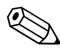
Si vous n'appuyez pas sur la touche **F10** au moment opportun, vous devrez redémarrer l'ordinateur et appuyer de nouveau sur la touche **F10** pour avoir accès à l'utilitaire.

3. Utilisez les touches de direction pour sélectionner **Set Supervisor Password (Définir mot de passe Superviseur)** et appuyez sur **Entrée**.
4. Saisissez un mot de passe superviseur et appuyez sur **Entrée**.
5. Redémarrez l'ordinateur. Sous Windows, cliquez sur **Démarrer > Arrêter l'ordinateur > Redémarrer**.
6. Appuyez sur une touche dès que vous voyez le message **Press any key to enter TPM Configuration (Appuyez sur une touche quelconque pour accéder à la configuration TPM)**.

7. Saisissez le mot de passe superviseur et appuyez sur **Entrée**.
8. Appuyez sur la touche **E** pour activer la puce TPM.

   La puce est à présent activée.

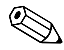
Initialisation de la puce de sécurité intégrée



Généralement, c'est l'administrateur du système informatique qui initialise la puce de sécurité intégrée.

1. Cliquez avec le bouton droit sur l'icône **HP ProtectTools** dans la barre d'état du système et cliquez sur **Embedded Security Initialization (Initialisation de la sécurité intégrée)**.

   L'assistant **HP ProtectTools Embedded Security Initialization** apparaît.
2. Cliquez sur **Suivant**.
3. Saisissez et confirmez un mot de passe Take Ownership (prise de possession), puis cliquez sur **Suivant**.



Entrez le mot de passe avec soin ; pour des raisons de sécurité, les caractères que vous saisissez n'apparaissent pas à l'écran.

4. Cliquez sur **Suivant** pour accepter l'emplacement par défaut du fichier de restauration ERA.
5. Saisissez et confirmez un mot de passe Emergency Recovery Token (clé de restauration de secours), puis cliquez sur **Suivant**.
6. Cliquez sur **Parcourir** pour sélectionner la destination appropriée.



ATTENTION : la clé de restauration de secours sert à récupérer les données chiffrées en cas de panne d'ordinateur ou de défaillance de la puce de sécurité intégrée. Les données chiffrées sont irrécupérables sans cette clé. (Les données sont également inaccessibles sans le mot de passe utilisateur.) Rangez cette clé dans un endroit sûr.

7. Cliquez sur **Save (Enregistrer)** pour accepter l'emplacement et le nom de fichier par défaut, puis cliquez sur **Suivant**.

8. Cliquez sur **Suivant** pour confirmer vos paramètres avant d'initialiser le système de sécurité.



ATTENTION : un message peut vous informer que les fonctions de sécurité intégrée ne sont pas initialisées. Ne cliquez pas dans la fenêtre de ce message, elle se ferme automatiquement au bout de quelques secondes.

9. Si le compte utilisateur doit être défini maintenant, vérifiez que la case à cocher **Start Embedded Security User Initialization Wizard (Lancer l'assistant d'initialisation des utilisateurs de la sécurité intégrée**) est cochée. Cliquez sur **Terminer**.

Définition d'un compte utilisateur

La définition d'un compte utilisateur :

- produit une clé utilisateur de base protégeant les données chiffrées
- définit une unité PSD pour stocker les fichiers et les dossiers cryptés

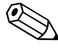


ATTENTION : gardez le mot de passe utilisateur en lieu sûr. Les données chiffrées sont inaccessibles ou irrécupérables sans ce mot de passe.

Pour définir un compte utilisateur de base et activer les fonctions de sécurité utilisateur, procédez comme suit :

1. Si l'**assistant d'initialisation des utilisateurs de la sécurité intégrée** n'est pas ouvert, cliquez avec le bouton droit sur l'icône **HP ProtectTools** dans la barre d'état du système, puis cliquez sur **Embedded Security User Initialization**.

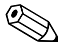
   L'assistant **HP ProtectTools Embedded Security Initialization** apparaît.
2. Cliquez sur **Suivant**.
3. Saisissez et confirmez un mot de passe utilisateur (Basic user), puis cliquez sur **Suivant**.



Entrez le mot de passe avec soin ; pour des raisons de sécurité, les caractères que vous saisissez n'apparaissent pas à l'écran.

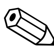
4. Cliquez sur **Suivant** pour confirmer.
5. Sélectionnez les fonctions de sécurité appropriées, puis cliquez sur **Suivant**.
6. Cliquez sur **Suivant** pour passer les fichiers d'aide.
7. Si plusieurs certificats de cryptage sont présentés, sélectionnez le certificat approprié.

   Cliquez sur **Suivant** pour appliquer le certificat de cryptage.
8. Définissez les paramètres appropriés de l'unité PSD, puis cliquez sur **Suivant**.
9. Configurer de nouveau l'unité PSD, puis cliquez sur **Suivant**.



La taille minimale de l'unité PSD est de 50 Mo ; la taille maximale est de 2 Go.

10. Cliquez sur **Suivant** pour confirmer.



La confirmation peut prendre plusieurs minutes, en fonction de la taille de l'unité PSD.

11. Cliquez sur **Terminer**.
12. Cliquez sur **Oui** pour redémarrer l'ordinateur.

Tâches courantes

Cette section présente les tâches élémentaires les plus fréquentes d'un utilisateur ou d'un propriétaire.

Tâches utilisateur

Les tâches élémentaires de l'utilisateur comprennent la configuration d'une unité PSD, le cryptage de fichiers et de dossiers, ainsi que l'envoi et la réception de courrier électronique chiffré ou signé numériquement.

Utilisation de l'unité PSD

Pour pouvoir utiliser l'unité PSD, vous devez entrer votre mot de passe. L'unité PSD apparaît alors et les fichiers sont déchiffrés. L'unité PSD s'utilise comme tout autre unité de disque.

Toutefois, lorsque vous n'en avez plus besoin, il convient de fermer la session. L'unité PSD est alors automatiquement masquée.

Cryptage des fichiers et des dossiers

Lorsque vous travaillez avec le système de fichiers EFS dans Windows 2000 ou dans Windows XP édition professionnelle, vous devez tenir compte de ce qui suit :

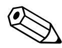
- Seuls les fichiers et les dossiers des partitions NTFS peuvent être chiffrés. (Les fichiers et les dossiers des partitions FAT ne peuvent pas être chiffrés.)
- Les fichiers système et les fichiers compressés ne peuvent pas être chiffrés et les fichiers chiffrés ne peuvent pas être compressés.
- Les dossiers temporaires devraient être chiffrés, étant donné que les fichiers temporaires peuvent présenter un certain intérêt pour les intrus.
- Des règles de restauration sont automatiquement définies lorsqu'un fichier ou un dossier sont chiffrés pour la première fois. De cette manière, si un utilisateur perd ses certificats et ses clés privées, il pourra se servir d'un agent de restauration pour déchiffrer ses données.

Pour chiffrer des fichiers et des dossiers :

1. Sélectionnez le fichier ou le dossier à chiffrer.
2. Cliquez avec le bouton droit de la souris ou du pavé tactile.
3. Cliquez sur **Encrypt (Chiffrer)**.
4. Cliquez sur **Apply changes to this folder only (Appliquer les modifications à ce dossier uniquement)** ou sur **Apply changes to this folder, subfolder and files (Appliquer les modifications à ce dossier, aux sous-dossiers et fichiers)**.
5. Cliquez sur **OK**.

Envoi ou réception de courrier électronique chiffré ou signé numériquement

Pour plus d'informations sur la signature numérique et le cryptage du courrier électronique, consultez l'aide en ligne de votre application de messagerie.



Pour pouvoir utiliser le courrier sécurisé, vous devez au préalable configurer votre application de messagerie pour qu'elle utilise le certificat numérique créé par l'utilitaire de sécurité intégrée. Si vous n'avez pas de certificat numérique, vous devez en obtenir un auprès d'un organisme de certification. Pour plus d'informations sur la configuration du courrier électronique et sur l'obtention d'un certificat numérique, consultez l'aide en ligne de votre application de messagerie.

Pour envoyer un message électronique chiffré, vous aurez besoin d'une copie de la clé publique ou du certificat numérique des destinataires. (Ce certificat contient une copie de la clé publique du destinataire.)

Microsoft Outlook utilise la clé publique du destinataire pour chiffrer le courrier ; vous ne devez donc pas introduire votre clé privée. Vous aurez toutefois besoin de votre clé privée pour lire un courrier chiffré, car le déchiffrement requiert la clé privée correspondant à la clé publique utilisée pour chiffrer le courrier.

Tâche de l'administrateur

L'administrateur peut effectuer un grand nombre de tâches dont certaines sont décrites ci-dessous. Pour plus d'informations, reportez-vous à l'aide de la sécurité intégrée HP ProtectTools.

Transfert des clés par l'assistant de migration de la sécurité de l'ordinateur

La migration est une tâche avancée de l'administrateur qui permet la gestion, la restauration et le transfert de clés et de certificats.

La première étape de la migration est l'autorisation, la configuration et la supervision du processus de transfert. Une fois l'autorisation accordée, l'utilisateur exporte et importe des clés et des certificats de l'ordinateur source vers l'ordinateur cible.

Pour plus d'informations sur la migration, reportez-vous à l'aide de la sécurité intégrée HP ProtectTools.

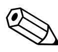
Restauration des informations

En cas de défaillance ou de réinitialisation de la puce de sécurité :

- L’assistant de restauration d’urgence permet de rétablir les données à partir de l’unité PSD.
- L’unité PSD est également compatible avec un agent de restauration qui est un mécanisme similaire au système EFS (Encryption File System).

  Pour savoir si vous disposez d’un agent de restauration sur votre ordinateur, cliquez sur **Démarrer > Tous les programmes > Outils d’administration > Stratégie de sécurité locale > Stratégies de clé publique > Agent de récupération de données cryptées**.

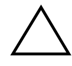
Pour plus d’informations, reportez-vous à l’aide en ligne du système d’exploitation.



Windows XP édition professionnelle ne crée pas automatiquement un agent de récupération. Pour définir l’agent de récupération, suivez la procédure indiquée dans l’aide du système d’exploitation.

Pour récupérer des données, l’agent de récupération doit accéder au certificat et aux clés numériques. Vous devez exporter le certificat de récupération et la clé privée sur disque et les garder dans un endroit sûr, puis supprimer la clé privée de récupération des données de l’ordinateur. La seule personne pouvant récupérer les données est celle qui a accès à la clé privée de récupération.

Rétablir la configuration d'usine de la puce de sécurité intégrée à l'aide de Computer Setup



ATTENTION : cette action supprime la définition de propriétaire de la puce de sécurité intégrée. Toute personne peut donc l'initialiser par la suite.

Si vous avez des fichiers cryptés, le rétablissement des paramètres d'usine de la puce de sécurité intégrée peut entraîner une perte de données.

Pour rétablir les paramètre d'usine de la puce de sécurité intégrée, procédez comme suit :

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter l'ordinateur > Redémarrer**.
2. Appuyez sur une touche dès que vous voyez le message **Press any key to enter TPM Configuration (Appuyez sur une touche quelconque pour accéder à la configuration TPM)**.
3. Saisissez le mot de passe superviseur et appuyez sur **Entrée**.
4. Appuyez sur la touche **C** pour effacer la puce TPM.
5. Appuyez sur la touche **Y** pour confirmer.

   La puce est à présent effacée.

Règles de bonne pratique

Si vous utilisez la sécurité intégrée, il est conseillé de suivre les directives :

- Un administrateur de la sécurité informatique devrait définir le mot de passe superviseur du BIOS dans Computer Setup et initialiser la puce de sécurité intégrée avant de mettre l'ordinateur à la disposition des utilisateurs.
- Un administrateur de la sécurité informatique devrait créer le fichier de restauration d'urgence (Emergency Recovery Archive) lors de l'installation de la solution de sécurité intégrée et inciter les utilisateurs à sauvegarder leur données régulièrement. En cas de défaillance du système, c'est la seule méthode permettant de récupérer des données cryptées. Le fichier d'archivage et la clé de restauration d'urgence devraient être stockés séparément.

- Le cryptage devraient s'appliquer à des dossiers et non à des fichiers individuels, de sorte que les fichiers temporaires générés lors de l'édition de documents soient également cryptés.
- Les données sensibles devraient être cryptées sur des ordinateurs faisant partie d'un domaine. Elles sont ainsi protégées contre des attaques cryptographiques hors ligne.
- L'ensemble du serveur sur lequel des données cryptées sont stockées devrait faire l'objet d'une sauvegarde régulière. De cette manière, en cas de restauration des données, les profils comprenant les clés de décryptage sont également restaurés.
- Si vous devez crypter (chiffrer) des types de fichier qui sont concernés par la restauration du système, placez-les dans un volume qui n'est pas affecté par la restauration du système.
- Le système ne prend pas en charge plusieurs niveaux de cryptage. Par exemple, un fichier EFS crypté ne devrait pas être placé sur l'unité PDS et un fichier déjà enregistré sur l'unité PSD ne devrait pas être crypté.

Questions fréquentes

Comment puis-je savoir que mon ordinateur est équipé d'une puce de sécurité intégrée HP ProtectTools ?

La puce est un composant matériel incorporé au système. Ce composant apparaît dans la liste du Gestionnaire de périphériques.

Où puis-je me procurer le logiciel de sécurité intégrée HP ProtectTools ?

Vous pouvez télécharger le logiciel, les drivers et l'aide en ligne en consultant le site HP à l'adresse http://www.hp.com/products/security.

Le logiciel de sécurité intégrée HP ProtectTools peut-il être désinstallé ? Comment ?

Oui. Le logiciel peut être désinstallé par la procédure standard de désinstallation de Windows. Avant la désinstallation, vous devez sauvegarder les données personnelles protégées par cryptage, sinon elles seront perdues. L'étape finale de la désinstallation consiste à désactiver la puce.

1. Allumez l'ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter l'ordinateur > Redémarrer**.
2. Appuyez sur une touche dès que vous voyez le message **Press any key to enter TPM Configuration (Appuyez sur une touche quelconque pour accéder à la configuration TPM)**.
3. Saisissez le mot de passe superviseur et appuyez sur **Entrée**.
4. Appuyez sur la touche **D** pour désactiver la puce TPM.

   La puce est à présent désactivée.

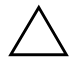
Résolution des problèmes

La sécurité intégrée ne fonctionne pas. Que dois-je faire ?

1. Cliquez avec le bouton droit sur l'icône **HP ProtectTools** dans la barre d'état du système et cliquez sur **Manage Embedded Security (Gestion de la sécurité intégrée)**.
2. Cliquez sur **Embedded Security > Info > Self Test (Autotest de la sécurité intégrée)**.

Vérifiez également sous **Embedded Security State (État de la sécurité intégrée), Chip (Puce), Owner (Propriétaire)** et **User (Utilisateur)**.

J'ai restauré mon système après un désastre. À présent, que dois-je faire ?



ATTENTION : dans la plupart des cas, c'est l'administrateur du système informatique qui exécute cette procédure. Si la procédure n'est pas exécutée convenablement vous pourriez perdre définitivement vos données.

Pour restaurer des données après remplacement de la puce ProtectTools, vous devez disposer de :

- SPEmRecToken.xml : clé de restauration de secours
- SPEmRecArchive.xml : dossier caché, situé par défaut dans C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive

- Les mots de passe ProtectTools
    - ❏ Superviseur
    - ❏ Prise de possession
    - ❏ Clé de restauration d’urgence
    - ❏ Utilisateur

1. Allumez l’ordinateur ou redémarrez-le. Sous Windows, cliquez sur **Démarrer > Arrêter l’ordinateur > Redémarrer**.
2. Appuyez sur une touche dès que vous voyez le message **Press any key to enter TPM Configuration (Appuyez sur une touche quelconque pour accéder à la configuration TPM)**.
3. Saisissez le mot de passe superviseur et appuyez sur **Entrée**.
4. Appuyez sur la touche **C** pour effacer la puce TPM.
5. Appuyez sur la touche **Y** pour confirmer.
6. Redémarrez l’ordinateur. Sous Windows, cliquez sur **Démarrer > Arrêter l’ordinateur > Redémarrer**.
7. Appuyez sur une touche dès que vous voyez le message **Press any key to enter TPM Configuration (Appuyez sur une touche quelconque pour accéder à la configuration TPM)**.
8. Saisissez le mot de passe superviseur et appuyez sur **Entrée**.
9. Appuyez sur la touche **E** pour activer la puce TPM.

   La puce est alors activée.
10. Une fois que Windows est lancé, cliquez avec le bouton droit sur l’icône **HP ProtectTools** dans la barre d’état du système et cliquez sur **Embedded Security Initialization (Initialisation de la sécurité intégrée)**.
11. Cochez la case à cocher : **I want to restore the existing Embedded Security (Je souhaite restaurer la sécurité intégrée existante)**, puis cliquez sur **Suivant**.
12. Tapez et confirmez un mot de passe de prise de possession. Cliquez sur **Suivant**.

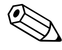
13. Cliquez sur **Do not create a recovery archive (Ne pas créer d'archives de restauration)**, puis sur **Suivant**.



ATTENTION : la création d'un nouveau fichier d'archivage détruit le fichier actuel nécessaire à la restauration, ce qui se traduit par la perte totale des données.

14. Cliquez sur **Yes (Oui)** pour continuer sans créer de nouveau fichier d'archivage.
15. Cliquez sur **Suivant** pour confirmer.
16. Cliquez sur **Parcourir** pour localiser le fichier d'archivage ; l'emplacement par défaut est : C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive\SPEmRecArchive.xml.
17. Cliquez sur **Ouvrir**, puis sur **Suivant**.
18. Cliquez sur **Parcourir** pour localiser la clé de restauration créée lors de **l'initialisation de la sécurité intégrée HP ProtectTools**, cliquez sur la clé, puis sur **Ouvrir**.
19. Tapez le mot de passe de la clé, puis cliquez sur **Suivant**.
20. Sélectionnez le nom d'ordinateur, puis cliquez sur **Suivant**.
21. Cliquez sur **Suivant** pour confirmer.

    Si un message vous informe que la restauration a échoué, revenez à l'étape 1. Vérifiez attentivement les mots de passe, l'emplacement et le nom de la clé, l'emplacement et le nom du fichier d'archivage.
22. Si le compte utilisateur doit être défini maintenant, vérifiez que la case à cocher **Start Embedded Security User Initialization Wizard (Lancer l'assistant d'initialisation des utilisateurs de la sécurité intégrée)** est cochée. Cliquez sur **Terminer**.



Les étapes 23 à 35 réinstallent la configuration d'origine pour l'utilisateur de base. Ces étapes doivent être répétées pour chaque utilisateur.

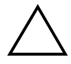
23. Si l'**assistant d'initialisation des utilisateurs de la sécurité intégrée** n'est pas ouvert, cliquez avec le bouton droit sur l'icône **HP ProtectTools** dans la barre d'état du système, puis cliquez sur **Restore Embedded Security Features (Restaurer les fonctions de sécurité intégrée)**.

    L'**assistant d'initialisation des utilisateurs de la sécurité intégrée** apparaît.

24. Cliquez sur **Suivant**.
25. Cliquez sur **Recover your basic user key (Restaurer la clé de base)**, puis sur **Suivant**.
26. Sélectionnez un utilisateur, saisissez le mot de passe de la clé de secours de cet utilisateur, puis cliquez sur **Suivant**.
27. Cliquez sur **Suivant** pour confirmer vos modifications et accepter l'emplacement des données de restauration.
28. Sélectionnez les fonctions de sécurité appropriées, puis cliquez sur **Suivant**.
29. Cliquez sur **Suivant** pour passer les fichiers d'aide.
30. Si plusieurs certificats de cryptage sont présentés, sélectionnez le certificat approprié.

    Cliquez sur **Suivant** pour appliquer le certificat de cryptage.

31. Le cas échéant, cliquez sur **I want to change my Personal Secure Drive settings (Je souhaite modifier mes paramètres d'unité PSD)**, puis sur **Suivant**.
32. Confirmez les fonctions de sécurité appropriées, puis cliquez sur **Suivant**.
33. Confirmez les paramètres, puis cliquez sur **Suivant**.
34. Tapez le mot de passe de l'unité PSD, puis cliquez sur **OK**.
35. Cliquez sur **Terminer** et sur **Oui** pour redémarrer.



ATTENTION : gardez le mot de passe utilisateur en lieu sûr. Les données chiffrées sont inaccessibles ou irrécupérables sans ce mot de passe.

Glossaire

Organisme de certification : service qui émet les certificats requis pour une infrastructure à clé publique.

Cryptographie : utilisation et étude du cryptage (chiffrement) et du décryptage (déchiffrement) ; les données sont codées de manière à ne pouvoir être décodées que par certaines personnes. Un système cryptographique est un système de cryptage et de décryptage. Ces systèmes font appel à un algorithme qui combine les données originales (texte ordinaire) avec un ou plusieurs nombres ou chaînes de caractères (clés) qui sont connus de l'expéditeur et du destinataire uniquement. Le résultat est du “texte chiffré” ou “texte crypté”.

Fournisseur de services cryptographiques : fournisseur ou bibliothèque d'algorithmes de cryptographie qui peuvent être utilisés dans une interface donnée pour exécuter des fonctions cryptographiques.

Décryptage : (déchiffrement) toute procédure utilisée en cryptographie pour convertir du texte crypté en texte ordinaire.

Certificats numériques : légitimation confirmant l'identité d'une personne ou d'une société en reliant l'identité du propriétaire du certificat numérique à une paire de clés électroniques utilisées pour signer des informations numériques.

Signature numérique : fonction utilisée pour vérifier l'identité de l'expéditeur d'un document numérique et certifier que le contenu de ce document n'a pas été modifié après que l'expéditeur l'ait signé.

Archivage pour la restauration de secours : emplacement de stockage protégé qui permet le recryptage des clés d'un utilisateur d'une plate-forme à une autre à partir d'une clé de propriétaire.

Cryptage (chiffrement) : p.ex. algorithme de cryptage ; toute procédure de cryptographie utilisée pour convertir du texte ordinaire en texte chiffré afin d'empêcher toute personne autre que le destinataire d'en lire le contenu. Il existe différentes méthodes de cryptage des données qui constituent la base de la sécurité des réseaux. Parmi les méthodes les plus utilisées, on trouve le DES (Data Encryption Standard) et le cryptage par clé publique.

EFS (Encryption File System) : système permettant de crypter tous les fichiers et sous-dossiers d'un dossier particulier.

Migration : tâche qui permet la gestion, la restauration et le transfert de clés et de certificats.

PSD (Personal Secure Drive) : unité sécurisée offrant une capacité de stockage protégée pour les données sensibles.

PKI (Public Key Infrastructure) : norme qui définit les interfaces de création, d'utilisation et d'administration des certificats et des clés de cryptage.

TPM (Trusted Platform Module) : ce module sécurisé est la mise en œuvre matérielle de la sécurité des données. Intégrée au système, la puce de sécurité intégrée peut vérifier l'intégrité du système et authentifie les utilisateurs tiers qui accèdent à la plate-forme, tout en restant totalement sous contrôle de l'utilisateur principal.